Sommaire de gestion

Rapport initial du groupe de travail du GNSO (organisation d'appui pour les noms de domaine génériques) sur l'hébergement 'fast flux'

STATUT DE CE DOCUMENT

Ceci est le sommaire de gestion du rapport initial du groupe de travail sur l'hébergement 'fast flux'.

Note de traduction

Ce document a été traduit de l'anglais pour atteindre un plus grand public. Bien que la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN) ait déployé des efforts pour vérifier la fidélité de la traduction, l'anglais est la langue de travail de l'ICANN et la version originale en anglais de ce document est le seul texte officiel et faisant autorité. Veuillez noter que ce sommaire de gestion constitue un seul chapitre du rapport complet uniquement disponible en anglais sur http://gnso.icann.org/ .

TABLE DES MATIERES

1 Sommaire de gestion

1.1. Contexte

- Suite à la publication de la recommandation du SSAC (Security and Stability Advisory Committee - Comité consultatif sur la sécurité et la stabilité) sur l'hébergement 'fast flux' et le DNS (SAC 025) en janvier 2008, le conseil du GNSO a enjoint à l'équipe ICANN le 6 mars 2008 de préparer un rapport sur les problèmes qui 'prendra en compte la recommandation SAC (SAC 025) et définira les prochaines étapes potentielles en matière d'élaboration des politiques GNSO visant à limiter la capacité actuelle des criminels à exploiter le DNS via les IP 'fast flux' ou les changements de serveurs de noms'
- Publié le 31 mars 2008, le rapport sur les problèmes recommandait que "le GNSO parraine les enquêtes et recherches supplémentaires afin d'élaborer les directives liées aux meilleures pratiques concernant l'hébergement 'fast flux' avant de considérer une mise en œuvre ou pas d'une procédure officielle d'élaboration de politiques".
- Lors de sa réunion du 8 mai 2008, le conseil du GNSO a officiellement lancé une procédure d'élaboration de politiques (PDP) et a demandé la création d'un groupe de travail sur le 'fast flux'. La charte du groupe de travail fut approuvée le 29 mai 2008. Elle demandait au groupe de travail de considérer les questions suivantes:
  - À qui bénéficie le 'fast flux' et qui en pâtit?
  - À qui bénéficierait l'arrêt de cette pratique et qui en pâtirait?
  - Les opérateurs de registres sont-ils ou pourraient-ils être impliqués dans des activités d'hébergement 'fast flux'? Si oui, comment?
  - Les bureaux d'enregistrement sont-ils impliqués dans les activités d'hébergement 'fast flux'? Si oui, comment?
  - Quelles sont les conséquences de l'hébergement 'fast flux' pour les titulaires de noms de domaine?
  - Quelles sont les conséquences de l'hébergement 'fast flux' pour les utilisateurs d'Internet?
  - Quelles sont les mesures techniques (telles que des modifications du fonctionnement des mises à jour du DNS) et stratégiques (telles que des modifications des accords registre/bureau d'enregistrement ou des règles régissant

les actions autorisées de la part des titulaires de noms de domaines) à mettre en œuvre par les registres et les bureaux d'enregistrement afin de limiter les effets négatifs du 'fast flux'?

- Quel serait l'impact (positif ou négatif) de la mise en place de limites, de directives ou de restrictions applicables aux titulaires de noms de domaine, aux bureaux d'enregistrement et/ou registres, en matière de pratiques permettant ou facilitant l'hébergement 'fast flux'?
- Quel serait l'impact de ces limites, directives, ou restrictions sur l'innovation en matière de produits et de services?
- Quelles sont certaines des meilleures pratiques disponibles en matière de protection contre le 'fast flux'?

Le groupe a été également chargé de recueillir l'avis d'experts, si nécessaire, afin de déterminer les aspects du 'fast flux' entrant ou non dans le cadre de l'élaboration des politiques du GNSO.

1.2. Approche adoptée par le groupe de travail

- Le Groupe de travail 'fast flux' a démarré ses délibérations le 26 juin 2008 et a décidé de commencer par répondre aux questions de la charte en parallèle à l'élaboration des déclarations de regroupements à ce sujet. Pour faciliter le retour d'information de la part des regroupements, un modèle fut élaboré pour les réponses (voir annexe I). En plus des conférences téléphoniques hebdomadaires, un dialogue de grande envergure regroupant plus de 800 messages publiés, fut établi à travers la liste de diffusion 'fast flux'.
- Sauf indication contraire, les positions brièvement exposées dans ce document devraient être considérées admises par le groupe de travail. Lorsqu'un large consensus ne pouvait être atteint, les marqueurs suivants ont été utilisés pour indiquer le niveau d'appui d'une certaine position:
  - Appui - plusieurs opinions positives ont été recueillies, mais des positions contraires peuvent exister et un large consensus n'a pas été atteint.
  - Point de vue alternatif - une opinion divergente a été exprimée, sans pour autant recueillir un appui suffisant au sein du WG pour mériter la qualification d'appui ou de consensus. Il faudrait noter qu'un point de vue alternatif pouvait être exprimé aussi bien dans le cas d'un large consensus que d'un appui.

1.3. Débat autour des questions de la charte

- Dans l'optique qui intéresse le groupe de travail, un réseau d'attaque 'fast flux' présente les caractéristiques suivantes:
  - Certains mais pas nécessairement tous les nœuds de réseaux sont opérés sur des hôtes compromis (c.-à-d. en utilisant un logiciel qui a été installé sur les hôtes sans préavis ou consentement de l'opérateur/propriétaire du système);
  - Il est 'volatile' dans le sens que les nœuds actifs du réseau changent afin de rendre possible la durée de vie du réseau, de faciliter la diffusion des composants du logiciel du réseau, et de mener d'autres attaques; et
  - Il utilise une variété de techniques pour atteindre la volatilité, y compris:
    - une sélection de systèmes rapide et répétée à partir d'une réserve d'hôtes robotés, l'utilisation de ces systèmes visant à servir des contenus malveillants, pour les utiliser comme serveurs de noms de domaine, et à d'autres fins, le tout par le biais d'enregistrements DNS à TLL réduites;
    - la diffusion de nœuds de réseau à travers un nombre considérable de systèmes autonomes de consommation;
    - la surveillance des nœuds membres pour déterminer/conclure qu'un hôte a été identifié et pour fermer; et
    - les changements de topologie de nœuds de réseaux, de serveurs de noms, de cibles proxy ou autres composants, basés sur le temps ou métriques.

    Les caractéristiques supplémentaires qui ont été utilisées en combinaison ou collectivement pour distinguer ou 'identifier l'empreinte digitale' d'une attaque d'hébergement 'fast flux' comprennent:
    - des adresses IP multiples par NS (serveur de noms), s'étendant sur de multiples ASN (numéros de systèmes autonomes),
    - des changements fréquents de NS,
    - des in-addrs.arpa ou IP situés dans des blocs d'attribution à large bande,
    - l'âge du nom de domaine,
    - des WHOIS de mauvaise qualité,
    - la détermination que le proxy nginx est exécuté sur la machine par adresse: le nginx est communément utilisé pour cacher des serveurs Web proxy (mandataires) illégaux,

  - le nom de domaine est éventuellement l'un parmi plusieurs noms de domaine au nom d'un titulaire dont le compte d'administration de domaine a été compromis, et l'attaquant a modifié les informations des noms de domaine sans y avoir été autorisé.

- La distribution et l'utilisation de logiciels installés sur les hôtes sans préavis ou consentement de l'opérateur/propriétaire du système constitue une caractéristique extrêmement importante d'un réseau d'attaque 'fast flux'; en particulier, il s'agit de l'une des caractéristiques qui distinguent les réseaux d'attaque 'fast flux' des utilisations productives des techniques 'fast flux' dans des applications telles que la mise en réseau de distribution de contenu, la mise en réseau à haute disponibilité et élastique, etc.
- Lorsqu'il est utilisé par des criminels, l'objectif principal de l'hébergement 'fast flux' est de prolonger la période de temps au cours de laquelle l'attaque continue à être efficace. Il ne s'agit pas d'une attaque en soi - il s'agit du moyen utilisé par l'attaquant pour éviter la détection et frustrer la réaction à l'attaque.
- Le WG présente les réponses initiales suivantes aux questions de la charte mais souhaiterait insister sur le fait qu'un travail continu est requis dans les domaines suivants:
  - Une définition du 'fast flux' technique robuste et de processus,
  - Des techniques fiables pour détecter les réseaux 'fast flux' tout en maintenant un taux acceptable de faux positifs,
  - Des informations fiables quant à l'envergure et la pénétration des réseaux 'fast flux',
  - Des informations fiables quant à l'impact financier et non financier des réseaux 'fast flux'
- Questions de la charte:

1. <u>À qui bénéficie le 'fast flux' et qui en pâtit?</u>

À qui bénéficie le 'fast flux'?

- Aux organisations qui gèrent des réseaux extrêmement ciblables
- Aux réseaux de distribution de contenu
- Aux groupes de libre parole / de pression

Qui pâtit des activités de 'fast flux'?

- Le WG a noté que des dommages pouvaient survenir aussi bien des usages légitimes que malveillants des techniques 'fast flux', et, au cours de leurs discussions, les membres du WG ont eu du mal à maintenir une distinction claire entre les dommages survenant directement des techniques elles-mêmes et ceux survenant du comportement malveillant de "mauvais acteurs" qui peuvent utiliser le 'fast flux' comme une des nombreuses techniques servant à éviter la détection.
- Le WG n'a pas atteint un consensus concernant la culpabilité séparément identifiable de l'hébergement 'fast flux' en matière de dommages causés par un comportement malveillant, tout en reconnaissant la manière selon laquelle les techniques 'fast flux' sont utilisées pour prolonger une attaque.

2. À qui bénéficierait l'arrêt de cette pratique et qui en pâtirait?

Les parties qui bénéficient de l'arrêt de la pratique sont les mêmes que celles qui sont lésées lorsque le 'fast flux' est utilisé en faveur des réseaux d'attaque 'fast flux'. Le WG s'est donc concentré sur l'identification des parties lésées.

- Les individus dont les ordinateurs sont infectés par des attaquants et par conséquent utilisés pour héberger des moyens de transmission dans un réseau d'attaque 'fast flux'.
- Les entreprises et organisations dont les ordinateurs sont infectés et par conséquent aptes à héberger des moyens de transmission dans un réseau d'attaque 'fast flux'.
- Les individus qui reçoivent des courriels hameçons et sont attirés vers un site hameçon hébergé sur un réseau d'attaque 'fast flux' peuvent avoir leurs identités volées ou subir des dommages matériels sur leurs cartes de crédit, titres ou comptes en banque.
- Les fournisseurs d'accès à Internet (FAI) sont lésés lorsque leurs blocs à adresses IP et leurs noms de domaine sont associés à des réseaux d'attaque 'fast flux'. Un FAI peut également encourir des coûts de mutation de personnel et de ressources afin de surveiller et de traiter l'abus.
- La réputation d'un bureau d'enregistrement peut être lésée lorsque ses services d'enregistrement et d'hébergement DNS sont utilisés pour faciliter les réseaux d'attaque 'fast flux' qui utilisent des techniques 'double flux'. Un bureau

d'enregistrement peut également encourir des coûts de mutation de personnel et de ressources afin de surveiller et de traiter l'abus.
- Les entreprises et organisations qui sont hameçonnées par des sites Web fantômes hébergés sur des réseaux d'attaque 'fast flux'.
- Les individus ou les entreprises dont les vies ou les moyens d'existence sont touchés par les activités illégales encouragées à travers les réseaux d'attaque 'fast flux'.
- Les registres peuvent encourir des coûts de mutation de personnel et de ressources afin de surveiller et de traiter l'abus.

À qui l'utilisation des techniques 'fast flux' bénéficie-t-elle?
- Aux organisations qui gèrent des réseaux extrêmement ciblables
- Aux réseaux de distribution de contenu
- Aux organisations qui fournissent des voies de transmission de libre parole, de plaidoyers en faveur des minorités, de pensées révolutionnaires.
- Aux criminels, terroristes, et généralement, à toute organisation qui gère un réseau d'attaque 'fast flux'

Le WG reconnaît que les usages futurs de cette technologie peuvent être développés et qu'en conséquence, il est impossible d'énumérer tous les usages avantageux possibles de cette technologie.

3. Les opérateurs de registres sont-ils ou pourraient-ils être impliqués dans des activités d'hébergement 'fast flux'? Si oui, comment?

Dans sa déclaration de regroupements, le registre de regroupements fournit des notes détaillées concernant les options de techniques et de politiques à disposition des opérateurs de registres en matière d'hébergement 'fast flux' (voir annexe III).

4. Les bureaux d'enregistrement sont-ils impliqués dans les activités d'hébergement 'fast flux'? Si oui, comment?

- La majorité des bureaux d'enregistrement n'est pas impliquée dans les 'fast flux' ou 'double flux'
- Quant aux bureaux d'enregistrement auprès desquels des domaines 'fast flux' sont enregistrés par des scélérats, la vaste majorité est constituée par des participants involontaires aux projets
- Quelques bureaux d'enregistrement et plus souvent des revendeurs de services de bureaux d'enregistrement apparaissent faciliter les attaques de domaine 'fast flux'.
- Aucun bureau d'enregistrement n'a été poursuivi pour facilitation d'activités criminelles liées à des domaines 'fast flux', mais il y a eu des rapports d'enquête établissant un lien entre un bureau d'enregistrement accrédité par l'ICANN et un nombre considérable de domaines frauduleux comprenant des domaines 'fast flux'.

De plus, le rapport décrit un nombre de vecteurs d'attaque connus ainsi que des contre-mesures.

5. Quelles sont les conséquences de l'hébergement 'fast flux' pour les titulaires de noms de domaine?

Les titulaires de noms de domaine sont des cibles des attaquants 'fast flux' à la recherche de noms de domaine qu'ils peuvent utiliser pour faciliter les attaques 'double flux'. Les attaquants sont attirés par des domaines existants jouissant d'une réputation positive plutôt que par des domaines récemment enregistrés, étant donné que l'âge et l'historique sont devenus des facteurs examinés par les enquêteurs lorsqu'ils tentent de déterminer si un domaine est associé à des attaques 'fast flux'.

6. Quelles sont les conséquences de l'hébergement 'fast flux' pour les utilisateurs d'Internet?

Les utilisateurs d'Internet fournissent la matière première exploitée par l'hébergement 'fast flux' (ordinateurs personnels connectés à des réseaux à large bande compromis par

des logiciels malveillants), tout en constituant le public cible des sites Web promus au moyen de pourriels que 'fast flux' favorise.

7. Quelles sont les mesures techniques (telles que des modifications du fonctionnement des mises à jour du DNS) et stratégiques (telles que des modifications des accords registre/bureau d'enregistrement ou des règles régissant les actions autorisées de la part des titulaires de noms de domaines) à mettre en œuvre par les registres et les bureaux d'enregistrement afin d'atténuer les effets négatifs du 'fast flux'?

Le WG souhaite mettre l'accent sur le fait que le 'fast flux' a besoin d'une meilleure définition et de plus de recherches. Les idées sont ici présentées en tant qu'ébauche, ouverte à l'enregistrement des progrès graduels. Les solutions se déclinent en deux catégories selon le type d'implication attendu de la part de l'ICANN et de ses parties contractantes ou accréditées (registres et bureaux d'enregistrement des extensions génériques gTLD): celles qui nécessiteraient uniquement la mise à disposition d'informations supplémentaires ou plus précises, qui pourraient être utilisées (ou ne pas être utilisées) par d'autres parties prenant part à des activités de lutte anti-fraude et autres y liées, selon qu'elles le jugent nécessaires (collecte d'informations); et celles qui nécessiteraient ou du moins bénéficieraient d'un certain degré de participation active de la part de l'ICANN et/ou des registres et bureaux d'enregistrement à l'identification et la prévention de comportements frauduleux ou autres comportements "malveillants" (engagement actif).

- Collecte d'informations - les propositions de partage d'informations discutées comprennent les idées suivantes:
    - La mise à disposition d'informations supplémentaires non privées concernant les domaines enregistrés par le biais de requêtes basées sur le DNS;
    - La publication de résumés de volumes de complaintes uniques par bureau d'enregistrement, par TLD et par serveur de noms;
    - L'encouragement des FAI à orchestrer leurs propres réseaux;
    - L'élaboration d'initiatives conjointes, communautaires afin de faciliter le partage de données et l'identification de noms de domaine problématiques.

- Engagement actif - les idées discutées et se rapportant à l'engagement actif comprennent:
    - L'adoption de procédures de suspension de domaine accélérées en collaboration avec des enquêteurs / répondeurs certifiés;
    - La mise en place de directives pour l'utilisation de techniques spécifiques telles que les valeurs TTL très basses;
    - L'identification de serveurs de noms comme statiques ou dynamiques dans les enregistrements de domaines par le titulaire de nom de domaine;
    - Le prélèvement d'une somme minime pour changements aux adresses IP statiques des serveurs de noms;
    - L'autorisation de la communauté Internet à limiter l'hébergement 'fast flux' d'une manière similaire à celle selon laquelle elle traite les autres abus;
    - Les procédures de vérification des titulaires de nom de domaine plus rigoureuses.

8. Quel serait l'impact (positif ou négatif) de la mise en place de limites, de directives ou de restrictions applicables aux titulaires de noms de domaine, aux bureaux d'enregistrement et/ou registres, en matière de pratiques permettant ou facilitant l'hébergement 'fast flux'?

Toute tentative de réponse à cette question de la part du WG est reportée jusqu'à ce que les prochaines déclarations de regroupements et les commentaires publics, spécialement requis sur ces points, aient été reçus et reconsidérés par le WG.

9. Quel serait l'impact de ces limites, directives, ou restrictions sur l'innovation en matière de produits et de services?

Toute tentative de réponse à cette question de la part du WG est reportée jusqu'à ce que les prochaines déclarations de regroupements et les commentaires publics, spécialement requis sur ces points, aient été reçus et reconsidérés par le WG.

10. Quelles sont certaines des meilleures pratiques disponibles en matière de protection contre le 'fast flux'?

Une source de meilleures pratiques en matière de protection contre le 'fast flux' peut être trouvée dans le monde de l'hameçonnage. Le groupe de travail anti-hameçonnage (APWG) a récemment publié un document de meilleures pratiques à mettre en œuvre par les bureaux d'enregistrement de domaines pour traiter les noms de domaine enregistrés par des hameçonneurs ("Anti-Phishing Best Practices Recommendations for Registrars" http://www.apwg.org/reports/APWG_RegistrarBestPractices.pdf). Plusieurs des pratiques brièvement exposées dans ce document s'appliquent directement ou indirectement au traitement des noms de domaines 'fast flux'.
De plus, la SAC 035 identifie des méthodes de réduction actuellement mises en œuvre par certains bureaux d'enregistrement, dans le cas où le bureau d'enregistrement fournit le DNS pour les domaines du client.

11. Recueillir l'avis d'experts, si nécessaire, afin de déterminer les aspects du 'fast flux' entrant ou non dans le cadre de l'élaboration des politiques du GNSO.

Certains membres du groupe de travail ont fourni des raisons soutenant que l'élaboration de politiques pour aborder le 'fast flux' n'entrait pas dans le cadre des attributions de l'ICANN, alors que d'autres membres étaient d'un avis différent. Les enquêtes et le travail du groupe de travail sur les définitions décrivent comment le 'fast flux' implique des questions d'utilisation de noms de domaine plutôt que des questions d'enregistrement de noms de domaine.

1.4. Enjeux

Bien que le groupe de travail ait mené son travail avec grand enthousiasme et avec dévouement, il a rencontré un nombre d'enjeux brièvement présentés au chapitre six, tels que l'absence d'une définition consacrée du 'fast flux' et de données annexes, et, les idées fausses concernant le champ d'application d'un PDP et les attributions de l'ICANN.

1.5. Conclusions provisoires

- Le fait d'atteindre une perception commune et une compréhension élargie des motivations sous-jacentes à l'emploi de techniques 'fast flux' ou de mise en réseau adaptative s'est avéré un problème particulièrement épineux pour le WG. Les tentatives

pour associer des intentions autres que criminelles et caractériser l'hébergement 'fast flux' de légitime ou illégal, bon ou mauvais, ont stimulé des débats animés.

- L'étude entreprise par des membres du WG a révélé que l'hébergement 'fast flux' est nécessairement et précisément caractérisé de "flux rapide" mais que, plus en général, l'hébergement 'fast flux' couvrait plusieurs variations et adaptations de techniques de mise en réseau sensibles aux évènements, dynamiques ou volatiles.
- Le WG admet que le 'fast flux' et les techniques similaires sont de simples composantes du problème plus étendu de fraude et d'abus d'Internet. Les techniques décrites dans ce rapport ne représentent qu'une partie d'une immense trousse à outils en constante évolution à disposition des attaquants: limiter toute technique que ce soit n'éliminerait pas la fraude et l'abus d'Internet.
- Ces diverses questions étroitement liées doivent être toutes prises en compte dans toute procédure potentielle d'élaboration de politiques et/ou dans toutes démarches suivantes. Le rôle que l'ICANN peut et devrait tenir dans cette procédure doit être méticuleusement examiné.

1.6. Étapes suivantes possibles

Note: le groupe de travail souhaiterait proposer les idées suivantes à la discussion et au retour d'information au cours de la période de commentaires publics. Veuillez noter qu'à ce stade, le groupe de travail n'a pas encore atteint de consensus sur les idées présentées ci-dessous. L'objectif du groupe de travail sera de reconsidérer les contributions reçues au cours de la période de commentaires publics et de déterminer, le cas échéant, quelles recommandations reçoivent l'appui du groupe de travail et peuvent être inclues dans le rapport final.

- Redéfinir le problème et le champ d'application en élaborant une nouvelle charte ou explorer d'autres recherches et enquêtes avant l'élaboration d'une nouvelle charte.
- Explorer l'éventualité d'impliquer d'autres parties prenantes dans la procédure d'élaboration de politiques 'fast flux'.
- Explorer d'autres moyens d'aborder le problème au lieu d'une procédure d'élaboration de politiques.
- Mettre l'accent sur les solutions / recommandations qui pourraient être abordées par l'élaboration de politiques, les meilleures pratiques et/ou les solutions de l'industrie.

- Considérer si les dispositions des politiques relatives aux abus d'enregistrement pourraient aborder le 'fast flux' en donnant le pouvoir aux registres / bureaux d'enregistrement de démonter un nom de domaine impliqué dans des activités 'fast flux'.
- Explorer l'éventualité d'élaborer un système de signalement de données 'fast flux' (FFDRS).